Department of Homeland Security Daily Open Source Infrastructure Report for 28 May 2008

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

- The Associated Press reports that a new Government Accountability Office (GAO) report finds that gaps in port security make the U.S. vulnerable to a terrorist attack. (See item **11**)
- ComputerWorld reports that a penetration tester was able to hack into a major FBI database in six hours using lapses in infrastructure design and patch management. (See item **34**)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams

Service Industries: Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities

Sustenance and Health: Agriculture and Food; Water; Public Health and Healthcare

Federal and State: Government Facilities; Emergency Services; National Monuments and Icons

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *May 27, Reuters* – (National) **Enterprise Independence natgas line repairs continue.** The Independence Hub natural gas production platform in the Gulf of Mexico remained shut in as repairs on the related Independence Trail pipeline continued, Independence's majority owner said Tuesday. Despite energy market rumors that the platform had restarted and some volumes were flowing on the pipeline, an Enterprise Products Partners LP spokesman said the company was sticking to its latest estimate of the first half of June for restart. "Repairs are ongoing. The line is shut in and there are no volumes flowing," the spokesman said. A pipeline leak caused the deepwater platform to shut in early April.
   Source: http://www.reuters.com/article/rbssEnergyNews/idUSN2737446120080527

2. *May 27, Agence France-Presse* – (Iowa; Minnesota) **Tornadoes rake U.S. Midwest.**

Authorities across the U.S. Midwest braced for the possibility of new deadly tornadoes Monday, after twisters swept through the region over the weekend. Marble-sized hail fell over the town of Waterloo, Iowa, where authorities reported significant damage to homes, trees, and power lines, CNN reported. The governor of Iowa declared a state of disaster in three counties. Meanwhile, in Minnesota, a separate twister struck the Minneapolis-Saint Paul area.
Source: http://newsinfo.inquirer.net/breakingnews/world/view/20080527-139057/8-killed-as-tornadoes-rake-US-Midwest----reports

3. *May 26, KIRO 7 Seattle* – (Washington) **Contaminated gas causes cars to stall.** Three or more gas stations had to shut down after contaminated fuel was pumped into several cars and trucks. At least nine cars and trucks broke down after the gasoline and water mixture was pumped into their vehicles, reported KIRO 7 Eyewitness News. The contaminated fuel was linked to a Shell facility on Harbor Island, said a spokesman for Shell Puget Sound Refinery. In a statement released by the Shell station in Snohomish, a preliminary investigation showed that human error at the Shell's Seattle terminal allowed gasoline mixed with water to be loaded onto delivery trucks. The contaminated regular unleaded gas was delivered to four Shell stations in the Seattle area, said the statement. The bad gas was only loaded into one tank, said Shell, and is not related to any of their other refinery operations.
Source: http://www.kirotv.com/money/16395366/detail.html

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

4. *May 27, Reuters* – (Connecticut) **Dominion Conn. Millstone 2 reactor remains shut.** Dominion Resources Inc. tried to start Unit 2 at the Millstone nuclear power station in Connecticut over the weekend but put the unit back in hot standby due to the loss of off-site power, the company told the U.S. Nuclear Regulatory Commission in a report. With the unit at one percent power, operators declared an unusual event on May 24 due to the loss of off-site power. The plant exited the unusual event on May 25 after workers restored the power. The unit shut May 22 likely due to a disturbance in the power grid caused by a lightning strike to a transmission line.
Source: http://www.reuters.com/article/marketsNews/idUSN2737057820080527

[Return to top]

Defense Industrial Base Sector

5. *May 27, TriState Observer* – (National) **Civil Air Patrol aids national preparedness.**

Civil Air Patrol (CAP) members on both coasts are participating in Ardent Sentry 08, a homeland security and disaster response exercise that tests the readiness of local, state, and national organizations responding to national-level emergencies, including both natural disasters and terrorism incidents. The East Coast exercise is involving CAP resources in the Middle East region. Responsibilities for CAP members include airborne reconnaissance and communications tasks, as well as other high-frequency communications support for Air Force North resources. The West Coast exercise is involving Pacific Region with a primary focus on Washington and Oregon Wings. Responsibilities are the same airborne and communications tasks as the East Coast exercise. According to the U.S. Northern Command Web site, exercise scenarios include multiple terrorist attacks in the state of Washington, an accidental chemical agent release in Oregon, and a Category 4 hurricane impacting the mid-Atlantic Coast.
Source: http://www.tristateobserver.com/modules.php?op=modload&name=News&file=article&sid=10063

6. *May 26, Associated Press* – (National) **U.S. bullets may be ill-suited for new wars.** The smaller, steel-penetrating M855 rounds continue to be a weak spot in the American arsenal. They are not lethal enough to bring down an enemy decisively, and that puts troops at risk, according to Associated Press interviews. Designed decades ago to puncture a Soviet soldier's helmet hundreds of yards away, the M855 rounds are being used for very different targets in Iraq and Afghanistan. Much of today's fighting takes place in close quarters; narrow streets, stairways, and rooftops are today's battlefield. In 2006, the Army asked a private research organization to survey 2,600 soldiers who had served in Iraq and Afghanistan. Nearly one-fifth of those who used the M4 and M16 rifles wanted larger caliber bullets. Yet the Army is not changing. The answer is better aim, not bigger bullets, officials say. In response to complaints from troops about the M855, the Army's Picatinny Arsenal in New Jersey assigned a team of soldiers, scientists, doctors, and engineers to examine the round's effectiveness. The team's findings, announced in May 2006, concluded there were no commercially available rounds of similar size better than the M855. Studies are being conducted to see if it can be made more lethal without violating the Hague Convention, Picatinny officials said. Larger rounds are not necessarily better, they also said. Other factors such as the weather, the amount of light, and the bullet's angle of entry also figure into how lethal a single shot may be.
Source: http://www.msnbc.msn.com/id/24828356/

[Return to top]

Banking and Finance Sector

7. *May 27, Salt Lake Tribune* – (National) **D.A.: Rearrest fraud suspect.** The U.S. district attorney wants to rearrest a man accused of creating a fake bank in Utah and taking millions of dollars from banks, investors and casinos nationwide, even while he was in jail. The suspect surrendered to the FBI in March after he allegedly tried to buy part of a Utah company with a $535,000 counterfeit check. He was released after a detention hearing and his assurances to make good on the payment. The scheme now appears to be

part of a complex web of phony bank transactions backed by fake cashier's checks, according to U.S. District Court documents. Authorities say the illegal acts continued after the man's release. More than 50 victims have been identified, and authorities think there may be more. The plot started in November 2007, when the man created the First Mutual Bank, portraying it on a Web site as an international bank based in London with locations in New York, Los Angeles and Salt Lake City. First Mutual and several other false banks with similar names were based in South Jordan and never were legitimate. The man allegedly printed three boxes of cashier's checks in the First Mutual name. Using a variety of schemes, he swindled collateral payments from banks, credit unions and at least one real estate investor. After his release, documents state, he "continued unabated," representing himself with a false name to new investors and reassuring others that he was not under investigation. On May 16, the U.S. Attorney's Office released the results of its continued investigation and asked that his release be revoked. The man, according to court documents, had committed similar crimes in Switzerland.
Source: http://www.sltrib.com/ci_9388897

8. *May 27, Pittsburgh Post-Gazette* – (Pennsylvania) **Scam artists play 'dialing for dollars.'** The latest telephone and text message scam to surface in Philadelphia spread into Wilkes-Barre and Scranton and then into Harrisburg, Pennsylvania. "It may be moving into your area next," said the deputy press secretary for Attorney General, referring to Pittsburgh and other cities and towns in Western Pennsylvania. "The scammers are using boiler rooms [no-frills call centers] and working their way through the state's area codes." The latest attempt to separate Pennsylvanians from their money is an international long-distance telephone scam with two variations: Consumers receive phone or text messages asking them to call what appears to be an ordinary long-distance number to confirm a lottery or sweepstakes prize. The other, more insidious variation of the scam asks consumers to call the number to get information about a relative who purportedly has been injured in an accident or is hospitalized. "Unsuspecting consumers who return these messages are actually calling international long-distance numbers, mainly in the Caribbean, and can be charged hundreds of dollars per minute for the calls," said the official. He said the crooks are taking advantage of the fact that some international numbers, such as 876 (Jamaica), 345 (the Cayman Islands), 284 (the British Virgin Islands) and 809 (the Dominican Republic), look like ordinary domestic area codes. Consumers should call directory assistance or an operator to check on the location for any unfamiliar number, and ask what the per-minute charges are for the number. They also should carefully review their monthly phone bills and immediately contact their phone company to dispute any unauthorized charges.
Source: http://www.post-gazette.com/pg/08148/885034-94.stm

9. *May 26, Examiner* – (District of Columbia) **D.C. finance office workers took thousands in funds, report says.** Employees in the District of Columbia's finance office helped themselves to thousands of dollars from an emergency cash fund that was supposed to help city workers, the Examiner has learned. Three employees, including a high-ranking finance official, have been fired in the wake of the scandal, sources familiar with an ongoing investigation said. Employees were taking petty cash from boxes around the city, the sources said. They were also keeping cash and checks from

payments back into the fund to cover themselves in case their drawers were short. The allegations are detailed in a report from the D.C. Auditor office that is still being drafted. The city's inspector general is also investigating. It is unclear how extensive the damage was. Records are scattershot, and the cash advance program did not have internal controls to spot trouble, the sources said.
Source: http://www.examiner.com/a-1408996~D_C__finance_office_workers_took_thousands_in_funds__report_says.html

10. *May 24, The Day* – (Connecticut) **Troopers' office warns of bank check scam.** The Montville, Connecticut, Resident Troopers' Office said citizens are receiving fraudulent bank checks for promising to return 10 percent of the funds to a third party. A Resident State Troop sergeant said phone solicitation is also on the rise, with parties calling to claim they are bank representatives. He said anyone who receives such a call should hang up and immediately call his or her bank branch directly.
Source: http://www.theday.com/re.aspx?re=adf15fbf-194d-42f3-871b-be0680adfb6d

[Return to top]

Transportation Sector

11. *May 27, Associated Press* – (National) **U.S. ports vulnerable to terrorists, probe finds.** A Government Accountability Office (GAO) report being released Tuesday finds that gaps in port security make the U.S. vulnerable to a terrorist attack. The report assesses the Customs-Trade Partnership Against Terrorism (C-TPAT), a federal program established after the September 11 attacks to deter a potential terrorist strike via cargo passing through 326 of the nation's airports, seaports and designated land borders. Under the program, roughly 8,000 importers, port authorities and air, sea and land carriers are granted benefits such as reduced scrutiny of their cargo in exchange for submitting a security plan that must meet U.S. Customs and Border Protection's minimum standards and allowing officials to verify their measures are being followed. Among the problems noted in the report were: A company is generally certified as safer based on its self-reported security information that Customs employees use to determine if minimum government criteria are met. But due partly to limited resources, the agency does not typically test the member company's supply-chain security practices and thus is "challenged to know that members' security measures are reliable, accurate and effective." Another problem is the fact that customs employees are not required to utilize third-party or other audits of a company's security measures as an alternative to the agency's direct testing, even if such audits exist. The GAO urged Customs and Border Protection to require consideration of third-party and other outside audits and take steps to make certain companies comply with any additional security improvements requested. The report calls for technological improvements to help improve consistency and better information-gathering in Customs' security checks. The Department of Homeland Security has said that while the likelihood of terrorists smuggling weapons of mass destruction into the U.S. in cargo containers is low, the nation's vulnerability and consequences of such an attack are potentially high.
Source: http://www.cnn.com/2008/US/05/27/port.security.ap/index.html

12. *May 27, Associated Press* – (Texas) **FBI: Pilot saw flaming object near Cleveland-bound jet.** A Continental Airlines pilot told air traffic controllers that an object with a flaming tail and a trail of smoke flew in front of the plane shortly after takeoff, FBI officials said. The FBI's Joint Terrorism Task Force is involved in the investigation, but officials said they believe the object seen by the pilot just east of Houston's airport on Monday was a model rocket. Officials are unsure how high the object flew or how close it came to the plane, a Federal Aviation Administration (FAA) spokesman said. The Boeing 737, which was carrying 148 passengers, was never in danger and landed safely, said a spokesman for the FBI's Cleveland office. Model rockets can reach up to 40,000 feet, although operators are supposed to notify the FAA if a rocket is entering controlled airspace, said an official with the Amateur Spaceflight Association in Houston.
Source: http://www.usatoday.com/travel/flights/2008-05-27-continental-object_N.htm

13. *May 27, Denver Post* – (Colorado) **Police close I-25 lanes to investigate terrorism threat.** The northbound lanes of Interstate 25 in Fountain, Colorado, were closed for nearly two hours early Monday morning while authorities searched a car for explosives. No explosives were found, said a Fountain police spokesman. Authorities received a warning through Pueblo police just before 3 a.m. about a possible terrorist action "against this country" involving someone in a red Chevrolet Geo. Fountain police stopped a driver, who was driving the red Geo north on I-25, the official said. A police dog indicated the car could have contained explosives. Northbound I-25 was closed from 4:20 to 6:15 a.m. at U.S. 85 in Fountain while members of the Colorado Springs Metro Explosives Unit processed the car. Investigators think that the man's statements in a call to Pueblo police, which led to the terrorist alert, might have been a result of his being under the influence of drugs or alcohol, the official said.
Source: http://www.denverpost.com/news/ci_9387413

14. *May 26, Detroit News* – (Michigan) **Unlocked door prompts brief lockdown at Metro Airport's McNamara terminal.** The Ed McNamara terminal at Detroit Metropolitan Airport was briefly shut down Monday afternoon, and passengers forced to stay in restricted areas, after security personnel discovered an unlocked door, an airport official said. Passengers were stranded for about 30 minutes while officials from the Transportation Security Administration (TSA) reviewed videotape to make sure no one had improperly gone through the door, said an airport spokesman. When the TSA was confident there was no security breach, passengers were free to move again, he said.
Source:
http://www.detnews.com/apps/pbcs.dll/article?AID=/20080526/METRO/805260390/1409/METRO

15. *May 26, Agence France-Presse* – (International) **Boeing 747 cargo plane crashes on take off at Brussels airport.** An American-owned Boeing 747 cargo plane crashed as it took off at Brussels airport, Belgium, on Sunday and broke apart, but the five-strong crew escaped without injury, airport officials said. The jumbo jet came to rest at the end of the runway some 500 yards from housing in the Brussels suburb of Zaventem after the crash. Local residents have long campaigned to have this particular runway shut down, and said the crash was entirely predictable. The plane broke into three pieces, and

stopped just meters short of electricity power cables. The massive four-engined jet belonged to Kalitta Air, an airport spokeswoman said. Belgian TV reported that the plane was carrying diplomatic baggage belonging to the U.S. Ambassador to Belgium, including a car and papers. The U.S. embassy in Brussels refused to comment. The five-strong crew were all Americans, and the plane was bound for the Gulf state of Bahrain, according to another airport official. No obvious cause for the crash was immediately apparent and an inquiry has been opened. Officials said the crash had not significantly affected air traffic, but the rail link between the airport and the centre of the Belgian capital had been suspended as the line ran close to the scene of the crash. Based in Michigan, Kalitta Air was founded in 2000 and has 18 Boeing 747s, according to its website.
Source: http://afp.google.com/article/ALeqM5h8e2_2N1_t8D2YPqSh8tw8qxQBig

16. *May 26, WESH 2 Orlando* – (Florida) **Southwest flight makes emergency landing.** Smoke caused a Southwest Airlines jet to make an emergency landing at Orlando International Airport on Sunday. Passengers on the flight from Norfolk, Virginia, to Orlando complained to staff of an electrical smoke smell. The smoke was coming from the jet's cockpit. Following the landing, the plane was towed to a terminal gate. Airline officials said maintenance crews are working to determine what caused the problem.
Source: http://www.wesh.com/travelgetaways/16393070/detail.html

17. *May 24, KOMO Newsradio Seattle* – (Washington) **Sea-Tac tightens security after incident.** Security procedures have been tightened at Seattle-Tacoma International Airport in Washington, following an incident in which a man was able to drive his van onto a runway without having his vehicle searched or his identity checked. The incident happened last week in an area reserved for corporate jets. At that time, there were no local or federal requirements to check IDs or screen vehicles at the entrance to the corporate terminal. After the incident, security officials took a look at their procedures, said a Sea-Tac spokeswoman. On Monday officials changed policies, and they no longer allow any vehicles on the tarmac, she said. Passengers now have their ID checked at the corporate gate and have to park their vehicle outside, then walk in.
Source: http://www.komoradio.com/news/local/19232199.html

[Return to top]

Postal and Shipping Sector

18. *May 26, Vero Beach Press-Journal* – (Florida) **Two Fort Pierce teens charged with making bombs.** Two Fort Pierce 19-year-old men were arrested late Friday for allegedly making homemade bombs and blowing up a mailbox. They were charged with using a destructive device to cause bodily harm or property damage and criminal mischief. According to an arrest report, one of the men told officers they were bored Friday evening, so they used some acid brought home from the swimming pool company where one works and a plastic bottle to make a small bomb, which they blew up in the street. Then they made a larger bomb, which they put inside a mailbox. The owner of the mailbox heard the explosion and called the Fort Pierce Police Department.
Source: http://www.tcpalm.com/news/2008/may/26/two-fort-pierce-teens-charged-

making-bombs/

[Return to top]

Agriculture and Food Sector

19. *May 27, Chicago Tribune* – (National) **Suspicions deepen on food labs.** A congressional committee is investigating whether some private U.S. laboratories were instructed to withhold samples of tainted food so that importers could get their goods into the U.S. In a May 1 letter to ten labs, the House Committee on Energy and Commerce suggests they may have been encouraged by importing companies to discard test results that had failed U.S. Food and Drug Administration (FDA) standards. The committee's letter reiterates one congressman's suspicion that testing on some samples was conducted repeatedly until the food passed. In some instances, the letter says, importers whose food failed tests at one laboratory would hire a different lab to continue testing until they got a positive result. "This repeated testing is done without alerting FDA that potentially dangerous food has been imported into this country – a practice which we find deplorable," the letter states. The committee asked 50 multinational food companies for a wide range of recall- and food-import records dating to 2000. So far, just two of the ten labs targeted by the House committee have complied with the records request, according to committee staffers.
Source: http://www.chicagotribune.com/news/chi-tainted-foodmay27,0,3491844.story

20. *May 27, Salt Lake Tribune* – (National) **Climate report adds more gloom.** On Wednesday, the U.S. Department of Agriculture released "The Effects of Climate Change on Agriculture, Land Resources, Water Resources and Biodiversity," a 200-plus page report that is part of a broader federal review of climate change. It had 38 authors, was reviewed by 14 scientists, and uses more than 1,000 references. "The report has more than 80 findings on the effects of climate change in the United States," a pre-release advisory said. The report, which focuses on the next 25 to 50 years, projects serious climate change related effect to agriculture, including rangeland that will not support cattle, streams too hot for trout, and forests felled by beetles and fire. The report can be found online at: www.climatescience.gov/Library/sap/sap4-3/default.php.
Source: http://www.sltrib.com/ci_9388903

21. *May 27, Bloomberg* – (National) **Corn costs signal biggest beef surge since 2003 as herds shrink.** The highest corn prices since at least the Civil War, based on Chicago Board of Trade data, mean U.S. feedlots are losing money on every animal they sell, discouraging production as rising global incomes increase meat consumption and a declining dollar spurs exports. Cattle may rise 13 percent by the end of the year on the Chicago Mercantile Exchange and Brazil's exchange, futures contracts show. Production also is dropping or failing to keep pace with demand in China, Brazil, and the European Union, mostly for grain-fed beef. The beef rally risks accelerating global food inflation, which has sparked riots from Haiti to Egypt. In the U.S., food prices will jump 5.5 percent this year, the fastest pace since 1989, according to the U.S. Department of Agriculture. As the incentive for producers dwindles, demand for U.S. beef exports will jump 14 percent next year. Sales will increase because of a declining dollar, rising

global incomes, and a relaxation of bans imposed after a case of mad-cow disease in 2003, the USDA said.
Source:
http://www.bloomberg.com/apps/news?pid=20601081&sid=axIrowbBQ7fo&refer=australia

[Return to top]

Water Sector

22. *May 26, Associated Press* – (California) **Water in Las Lomas has high mercury levels.** Officials are warning Las Lomas residents to refrain from drinking their tap water after tests found high mercury levels. The Monterey County Sheriff's Office says the contamination may have occurred when a storage tank that serves 3,000 residents, was vandalized on Saturday. Deputies responded to reports that vandals had broken into the water storage facility, and found a hatch had been forced open. The California Water Service Co. tested the water and found the high mercury levels. The company does not know when the water will be safe to drink again. No injuries have been reported.
Source: http://www.santacruzsentinel.com/localnews/ci_9388466

23. *May 25, Needles Desert Star* – (Arizona) **PG&E to drill new test wells to help monitor toxic plume.** In an ongoing effort to clean up a plume of contaminated groundwater near its Topock Compressor Station in California, Pacific Gas and Electric Co. will be drilling three to four new test wells along the Colorado River near Topock, Arizona. PG&E has been drilling test wells near its compressor station in California since before the plume of hexavalent chromium was discovered at a well near the Colorado River in 2004, but the new wells will mark the first time test wells have been drilled outside of California. Under the oversight of the Arizona Department of Environmental Quality, PG&E will install monitoring wells near and beneath the river to collect samples of groundwater and sediments. The samples will be collected for chemical analysis at each site as the wells are being drilled. Once the wells are completed, groundwater samples will be collected on a regular basis and be analyzed for chromium or other contaminants. According to the spokesman, the new wells will be able to provide specific information to help create a long-term plan that will be the most effective. While no long-term plan has been made, PG&E is taking interim measures to ensure that the Colorado River is not contaminated by the chemical plume. Under the direction of the California Department of Toxic Substance Control, PG&E is pumping 29,000 gallons of water per day out of the ground, treating it to remove the hexavalent chromium and then pumping it back into the ground near the river.
Source: http://www.mohavedailynews.com/articles/2008/05/25/news/local/local2.txt

24. *May 25, Sun News* – (South Carolina) **Contamination rages on years after base closes.** High levels of environmental contamination still exist at the former Myrtle Beach Air Force Base, South Carolina, more than 15 years after the military left, but experts say the pollution is not affecting new retail and residential developments there. The contamination also is not related to groundwater pollution discovered last year in a roughly 10-block neighborhood near the AVX Corp. manufacturing facility, which is

located adjacent to the base, according to state and federal officials. Environmental tests over the past three years show chemicals such as benzene, vinyl chloride and trichloroethylene, or TCE, exist in groundwater at the former military base at levels far above what the Environmental Protection Agency considers safe for drinking water. Environmental reports show one of the most polluted sites on the base is the former Petroleum, Oil and Lubricants Yard. The military used that site between 1955 and 1993 to store fuel in large above- and below-ground tanks. Groundwater tests at that site showed levels of benzene as high as 2,500 parts per billion in June, the most recent data available. Benzene levels at many of the POL Yard wells have fluctuated over the years. A hydrogeologist with DHEC said such fluctuations can be caused by changes in the water table, dry or rainy weather and other factors. Contaminated groundwater is slowly flowing toward a culvert that empties into the lake adjacent to The Market Common project, and state officials are monitoring the area to make sure contamination does not spread to the lake. There are about a half-dozen other sites where groundwater contamination far exceeds the EPA's safe levels. Groundwater at a site where the military used to mix pesticides, called the Old Entomology Shop, has levels of vinyl chloride as high as 442 parts per billion and now-banned pesticides at levels that exceed EPA standards, according to tests conducted in December 2006.
Source: http://www.myrtlebeachonline.com/news/local/story/462491.html

25. *May 25, The Sun* – (California) **Senator on the alert.** A California senator wants companies suspected of polluting Rialto's groundwater to pay for safe drinking water while a final cleanup strategy is devised. The water is contaminated with perchlorate, a chemical used to produce explosives like rocket fuel and fireworks. The perchlorate and a toxic industrial cleaner have spread into underground water, though contaminated water is not served to residents. Perchlorate can interfere with the thyroid gland, which plays a role in metabolism and mental and physical development. Rialto customers have a perchlorate surcharge on their water bills, and it costs hundreds of thousands of dollars a year to operate the treatment systems. In March, the senator wrote a letter to the Environmental Protection Agency administrator saying the agency should order suspected polluters to provide replacement water. The replacement water is particularly important as Rialto tries to build new residential developments that need water services, said a Rialto City councilman.
Source: http://www2.sbsun.com/sanbernardino/ci_9381286

26. *May 24, Associated Press* – (National) **EPA tests plans to protect water from terrorists.** Water utilities would get earlier warning of viruses, bacteria or chemicals that could be introduced into drinking water systems by terrorists under a test monitoring program set for expansion beyond Cincinnati. The pilot program ordered by the Department of Homeland Security in response to the September 11 terrorist attacks uses continuous monitoring of public water for contaminants that could sicken or kill millions of people. Some utilities only do spot checks now for such germs, pesticides or radioactive materials. Some utilities might find that they need additional video cameras and alarms to warn of intruders at water tanks or other sites. Once the pilot program is complete, the Environmental Protection Agency (EPA) hopes to have a national water security model that utilities could adopt at their own expense. The monitoring also could

detect unintentional contamination and could help utilities improve their overall water quality, said the project coordinator for the EPA's Water Security Initiative. Such contamination could include pollution from chemicals spills in lakes or rivers. The agency and the Greater Cincinnati Water Works began the $11 million test project in 2006, and it took about a year and a half to install the equipment, including sensors placed in the water distribution system at strategic points that feed information to computers for analysis. The system also calls for development of a network of labs to analyze water samples if there is suspected contamination and a computer program that would allow more comprehensive monitoring of consumer complaints, emergency calls and public health agency complaints for clues indicating a widespread problem. Source: http://ap.google.com/article/ALeqM5gqeMJT06_Wvi4W5d5Vr9gk5BuFfgD90RUG0O0

[Return to top]

Public Health and Healthcare Sector

27. *May 27, Canadian Press* – (International) **Study: Bird flu viruses adapting to humans.** North American avian flu viruses of the H7 subtype – like the one responsible for British Columbia's massive poultry outbreak in 2004 – seem to have adapted to more easily invade the human respiratory tract, suggests a new U.S. Centers for Disease Control (CDC) study published Monday by the journal Proceedings of the National Academy of Sciences. Experts say the findings underscore the fact that H7 flu viruses pose a significant pandemic threat and that surveillance for cases in wild birds, poultry, and people ought to be a high priority. CDC scientists tested the various viruses to see which types of receptors they can latch onto – those typically found in the guts of birds, the natural host of influenza viruses, or those found on the cells of the lining of the upper respiratory tract of humans. Human flu viruses that circulate every winter have adapted to bind to the receptors in the human respiratory tract, known as alpha 2-6 receptors. Avian viruses, on the other hand, prefer the alpha 2-3 receptors found in the guts of wild birds and poultry but which are scarce in the human upper respiratory tract. Source: http://thechronicleherald.ca/Canada/1058455.html

28. *May 26, FoodConsumer.org* – (National) **West Nile virus: National overview.** According to U.S. Geological Survey (USGS), five people in four states and 12 mosquito samples from two states have tested positive for West Nile as of May 23. The five human cases have been reported in Maricopa County (1) in Arizona, Montgomery County (1) in Texas, Lincoln County (1) and Madison County in Mississippi, and Shelby County (1) in Tennessee. There is often a delay that local and state governments report West Nile cases to the federal agency. Mosquito samples that tested positive for West Nile virus have been reported in Riverside County (9) in California and Harris County (3) in Texas as of May 20, according to the USGS. In California, the State Department of Public Health confirmed that as of May 23, West Nile activity had been found in ten counties. Compared to 2007, the virus seems more active this year. Source: http://foodconsumer.org/7777/8888/I_nfectious_D_idease_57/052611272008_West_Nil

e_time_National_overview.shtml

29. *May 25, Los Angeles Times* – (National) **Drug taken to stop smoking is linked to traffic mishaps.** The nonprofit Institute for Safe Medication Practices last week linked Chantix to more than two dozen highway accidents reported to the Food and Drug Administration, saying the mishaps may have resulted from such drug side effects as seizures. The FDA had earlier issued a warning about suicidal thoughts and suicides among patients taking Chantix and is now evaluating whether it needs to expand and strengthen that precaution. Pfizer, the drug's manufacturer, said that as early as May of last year, it had added a warning to the prescribing literature for Chantix that patients should exercise caution when driving or operating machinery until they know how the medication affects them. The Federal Aviation Administration continued, until last week, to list the drug as approved for pilots. The federal truck safety agency was also unaware of the risk. The military, which bans Chantix for flight and missile crews, is considering whether other precautions are needed, Pentagon officials said.
Source: http://www.latimes.com/features/health/la-na-smokedrug25-2008may25,0,4540550.story?page=1

Government Facilities Sector

30. *May 23, Examiner* – (District of Columbia) **District cops lose guns, drugs, money from evidence warehouse, audit says.** The Metropolitan Police Department (MPD) lost guns, drugs, and cash seized as evidence and jeopardized criminal prosecutions by failing to secure its evidence warehouse and databases, a scathing new audit finds. After inspecting the MPD's Evidence Control Branch, the D.C. inspector general (IG) concluded that the department "is not achieving its mission [of] preserving the integrity of evidence in its custody." Property records were in disarray, unauthorized personnel were allowed unregulated access to property vaults, evidence was lost, and no one could say who had access to the computerized evidence database. There is a "high risk that individuals may have inappropriate access and the ability to alter data without detection," the IG found. The evidence warehouse contains about two million items. Auditors sought to locate a sample of 120 from three categories – 40 each from weapons, drugs, and money – but failed to find more than a third.
Source: http://www.examiner.com/a-1405584~District_cops_lose_guns__drugs__money_from_evidence_warehouse__audit_says.html

[Return to top]

Emergency Services Sector

31. *May 27, Occupational Health & Safety* – (Virginia) **'Dirty bomb' test brings Virginia, federal agencies together.** A May 22 exercise in the Hampton Roads, Virginia, area brought state and federal responders together to simulate their response to a radiological release. The East Coast Initiative/U.S. Coast Guard Hampton Roads Area Maritime

Security exercise brought together Virginia's Office of Commonwealth Preparedness, the U.S. Navy's Center for Asymmetric Warfare, and the U.S. Coast Guard's Hampton Roads Area Maritime Security Committee to test procedures, resource deployment, and information sharing among the three organizations. Participants included the Virginia Fusion Center, Virginia Department of Emergency management, Virginia State Police, the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and the Federal Emergency Management Agency.
Source: http://www.ohsonline.com/articles/63268/

32. *May 25, Daily Advertiser* – (Louisiana) **Trains' cargo raises concern.** Every day, hazardous materials, including flammable gases and liquids, pass through Lafayette, Louisiana, by train, traveling next to homes and businesses, skirting the downtown area and passing within yards of the city's main utility plant. For safety reasons, railroad companies do not publicize the types or quantities of hazardous materials that they transport through communities like Lafayette. However, even first-responders like the Lafayette Fire Department's hazardous materials team do not know what is being transported through the city until an accident occurs, the city's fire chief said, adding that on May 17, when six cars of a train derailed there, spilling hydrochloric acid, the fire department's haz-mat unit learned what the train was carrying only when firefighters were on their way to the accident site. The director of the Lafayette Parish Office of Homeland Security and Emergency Preparedness said his office has no such list nor is there any need for his office to have a list of the top 25 chemicals transported by train through Lafayette.
Source: http://www.theadvertiser.com/apps/pbcs.dll/article?AID=/20080525/NEWS01/805250342/1002

33. *May 25, Lake County News* – (California) **Office of Emergency Services plans training exercise.** The Lake County Office of Emergency Services, in conjunction with its operational area cooperators, will conduct the second annual Mass Casualty Incident training exercise this week on Wednesday, May 28. The exercise will test Lake County's and the mutual aid partners' response to a hazardous materials/mass casualty incident on a major artery of Lake County, where there may be a fire involved and multiple injuries and fatalities. Although actual traffic on Highway 20 will not be affected, responders will coordinate the anticipated traffic congestion as if this were a real event. The fire, police, and emergency medical service representatives will effectively carry out their simulated response. Agencies outside of Lake County will support the execution of this exercise. The exercise will facilitate the training needed to ensure that emergency responses for hazardous materials, mass decontamination, and medical services are fully functional to protect the public and save lives and property in the event of an actual incident.
Source: http://lakeconews.com/content/view/4314/764/

[Return to top]

Information Technology

34. *May 27, ComputerWorld* – (National) **Six hours to hack the FBI.** A penetration tester at PatchAdvisor Inc. hacked his way into a major FBI crime database within a mere six hours. He used "security lapses in both infrastructure design and patch management." He said that during a routine network scan, he discovered a series of unpatched vulnerabilities in the civilian government agency's Web server, as well as other parts of the enterprise. He then used a hole in the Web server to pull down usernames and passwords that were reused on a host of enterprise systems. In those systems, he found further account details that allowed him to get Windows domain administrator privileges. Using this privileged access, he was able to gain full control of almost all Windows-based systems in the enterprise, including workstations used by the on-site police force. He noticed that several police workstations had a second networking card installed that used the SNA protocol to directly talk to an IBM mainframe. By covertly installing remote control software on those workstations, he found programs on their desktops that automatically connected the workstations to the FBI's NCIC database. "That software, coupled with a keystroke capture program, would allow an attacker to grab the credentials needed to log into the FBI's National Crime Information Center database," he says. Like most vulnerabilities he's found over his years of paid ethical hacking, this one could have easily been eliminated with some basic security strategies, he says. For instance, the police network should have been firewalled off from the main enterprise network, and the investigators' workstations kept out of the larger domain. Also, he says the agency should not have allowed those workstations both NCIC and general enterprise network access, since they were connected to something with such obvious national security implications. Finally, the system administrators should have monitored and blocked the common reuse of passwords.
    Source:
    http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9087441&pageNumber=1

35. *May 27, Reuters* – (International) **Hackers make way for criminals in cyberspace.** Attacking the European Union's Internet backbone is now the preserve of organized crime, not young hackers out to prove a point, the executive director of the European Network and Information Security Agency (ENISA) said, adding that public authorities have been able to hold their own in the contest – so far. There is a continuous struggle between the attackers and the increases in protection of information systems. "It's a contest," he told Reuters. The economy of the EU's 27 nations, like elsewhere in the world, increasingly depends on a trouble-free Internet to operate, but there have been reminders of what can go wrong. Last year, government websites in Estonia crashed with the Baltic state accusing Russia of being behind what many saw as the first major cyber attack in Europe. But with a budget of just $12.6 million a year and a staff of 50, ENISA needs more resources, ENISA's director added.
    Source:
    http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=208400171

36. *May 27, Search Engine Watch* – (International) **CAPTCHA hacks for Gmail, Blogspot, Craigslist causing problems.** Hackers seem to have found a way to work

around CAPTCHA – the once great hope of stopping bots from spamming. A Search Engine Watch Forum member noted that there are now programs being offered that work around the filter.
Source: http://www.hackinthebox.org/index.php?name=News&file=article&sid=26803

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

37. *May 27, Wall Street Journal* – (National) **Do hackers pose a threat to smart phones?** Like computers, smart phones are vulnerable to viruses and other types of malicious software. By all accounts, the risk of a smart-phone attack is low, but as people start using the devices for more sensitive tasks – handling customer data and transferring corporate files – security experts say smart phones may become more vulnerable. So companies are working to protect both the devices and the networks behind them. At the corporate level, IT departments are cracking down, mainly by limiting access these devices have to internal networks. On the consumer front, computer-security companies are selling antivirus software that scans for rogue applications. Smart phones are used mainly by professionals who want to access corporate email and send documents on-the-go. But the market for these high-end devices is growing. So far, there are about 300 to 500 known versions of malicious software, or malware, written for phones – a small number compared to those that attack personal computers. Malware infects phones through email attachments and text messages that ask users to download an application. They also can be delivered over wireless connections using Bluetooth technology. The majority of mobile malware has been written for phones using the Symbian operating system, which is found in about 65 percent of the global smart-phone market, according to ABI Research. Phones that run Symbian include some models made by Nokia, Samsung and Sony Ericsson. Regardless of the operating system, the greatest risk of infection comes from third-party applications, such as games and ringtones. Beyond downloading software only from trusted companies, individuals who own personal smart phones can protect themselves with antivirus software.
Source:
http://online.wsj.com/article/SB121184343416921215.html?mod=googlenews_wsj

38. *May 25, Financial Mail* – (International) **Huge security alert over BT broadband.** Hundreds of thousands of British Telecom (BT) broadband customers are at risk of massive breaches of their computer security because of a flaw in the Home Hub wireless network systems installed by the telecoms giant. BT has 4.4m broadband customers and it is believed most of those supplied with wifi boxes are vulnerable to hacking. Only the latest versions of the BT system are safe from attack. And though BT has been aware of

the problem for months, it has not written to customers to warn them of the risk and the simple fix. Computer experts last week demonstrated to Financial Mail how easy it was for a hacker to use a free computer program to join a household network without being told the password. It took five minutes for the program to probe the wi-fi hub and gain access. From there, more skilled computer criminals could access and seize vital personal data from individual computers.
Source:
http://www.thisismoney.co.uk/bbphone/article.html?in_article_id=442103&in_page_id=182&ct=5

[Return to top]

Commercial Facilities Sector

39. *May 27, Associated Press* – (Georgia) **ATF training to real threats.** Federal agents from the Bureau of Alcohol, Tobacco, Firearms and Explosives are taking part in a four day training exercise in Atlanta. The exercise is intended to demonstrate crime scenes ATF agents might encounter. "We're replicating devices that have actually been used in the United States," said an assistant agent in charge of the Atlanta field division of the ATF. "We're going to match our training to the threats that we're seeing." More than two dozen agents from around Georgia descended on an abandoned two-story brick apartment complex, nestled in woods about 30 miles east of downtown Atlanta. Accompanying them were two Labrador retrievers trained for explosives detection, a mobile laboratory and an RV version of a bomb response unit. Forensic chemists and other technicians pored over evidence to determine the explosive used and other details that could help solve the crime. Part of the exercise required agents to consider whether the victim was a bomber who accidentally set off his device, a roommate or some other innocent individual, an official said. Extremist literature was scattered about to provide clues in what was meant as a simulation of a homemade explosives lab. "It's naive to think that what's happened overseas will not happen here," said the assistant agent.
Source: http://www.onlineathens.com/stories/052708/news_20080527028.shtml

[Return to top]

National Monuments & Icons Sector

40. *May 25, KTBC 7 Austin* – (Texas) **Record crowds force closure of Travis County parks.** Texas Parks and Wildlife officials have had to close several parks around central Texas lakes as record numbers of crowds filled the parks to capacity. Mansfield Dam Park, Hippie Hollow, Bob Wentz Park, and Cypress Creek Park are all closed. Officials are turning people away because there is no more room. Officials believe that more people are deciding not to go on vacation and are going to local parks instead.
Source:
http://www.myfoxaustin.com/myfox/pages/News/Detail?contentId=6622345&version=2&locale=EN-US&layoutCode=TSTY&pageId=3.2.1

41. *May 24, Associated Press* – (Wisconsin) **Vandals damage Sept. 11 memorial at**

Memorial Park in Arcadia. Arcadia police were trying to determine who vandalized a memorial for the victims of the September 11 terrorist attacks at Memorial Park. A police chief said someone scratched words in English and Spanish in two large granite slabs that signify the fallen Twin Towers at the 54-acre park. The damage was found Wednesday night. A $10,000 reward is being offered for the arrest and conviction of the vandals.
Source: http://www.chicagotribune.com/news/chi-ap-wi-memorialdamage,0,5005015.story

[Return to top]

Dams Sector

42. *May 24, Chronicle* – (Washington) **Melting snow leads to extra spill at Chief Joseph Dam.** The U.S. Army Corps of Engineers is prepared to spill more water from Chief Joseph Dam in the next several days because of warmer temperatures and melting snow pack above Grand Coulee Dam. Officials planned to start spilling water from the Columbia River dam, located just below Grand Coulee, on May 24. Chief Joseph Dam is a "run of the river dam," said an official with the U.S. Army Corps of Engineers' Seattle district water management office in Seattle. That means water hitting the dam must go downstream, according to a Corps announcement. Once water exceeds the capacity of the powerhouse to generate electricity, extra water must go through spillway gates to maintain the desired pool level behind the dam, according to the official. Only a few of the spillway gates nearest the powerhouse are likely to be needed for the spill and that downstream effects will be minimal, she said.
Source: http://www.omakchronicle.com/nws/n080524a.shtml

43. *May 24, Huma Today* – (Louisiana) **Morganza review panel gets acquainted with levee system.** Seven scientists, professors, engineers and sociologists from across Louisiana spent most of Friday learning about Houma's proposed hurricane-protection system. The panel, directed by the state's Coastal Protection and Restoration Authority, was set up to ensure Morganza-to-the-Gulf maximizes hurricane protection with minimal environmental impact. Morganza is a system of levees, floodgates, locks and other structures designed to protect Terrebonne and western Lafourche from storm-related flooding. Terrebonne levee officials asked for the review in hopes of quelling criticism from environmentalists and scientists who question whether Morganza's proposed alignment would harm acres of eroding wetlands and argue that it would fail to provide adequate hurricane protection. On Friday, the panel got a board overview of Morganza and heard the types of scientific modeling used to study storm surges, storm waves and tidal circulation in the area. Specifics will be discussed in detail at future meetings, officials said. Morganza is designed to give a 100-year level of protection, one that aims to defend against surges from hurricanes with a 1 in 100 chance of hitting during any given year.
Source:
http://www.houmatoday.com/article/20080524/ARTICLES/805240316/1211/news01&title=Morganza_review_panel_gets_acquainted_with_levee_system

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer